ISO/IEC 27001:2022 Transition Plan for Clients

ISO 27001:2022, **"Information security, cybersecurity, and privacy protection — Information security management systems — Requirements,"** was released in October 2022 and is set to replace ISO 27001:2013 via a 3-year transition period. All organizations that wish to remain certified to ISO 27001 will need to transition to the 2022 revision of the standard within the set transition period, which is expected to end by 31st Oct 2025. The overall allowable transition period is expected to be 3 years (i.e., from October 2022 through October 2025).

ControlCase's goal is to maintain a clear transition plan that is easy for our clients to comprehend and apply. We aim to guide clients to make the transition from ISO 27001:2013 to ISO 27001:2022 as smooth as possible.

During that period, both versions of the ISO 27001 standard remain valid, and audits of either version may be conducted subject to the rules noted below. Still, plans should be made for an organization's transition to the 2022 version before the transition period ends.

Detailed Transition Period:

- **25th October 2022 -** ISO/IEC 27001:2022 3rd edition - **Release date**
- **Q4-2022** – ControlCase planned to start 2022 version audits by Q4-2023. Q3-2023 ControlCase expects ABs approval for 2022 version audits.
- **30th April 2024 -** All initial (new) certifications and all recertification audits should be to the 27001:2022 edition after this date.
- ControlCase will continue to accept applications for certification and issue new certificates against the 27001:2013 standard until this date.
- **31st July 2025 -** All transition audits should be conducted by this date.
- **31st October 2025 - Transition period ends** - Certificates for ISO/IEC 27001:2013 will no longer be valid after this date.

ISO/IEC 27001:2022 Revision Analysis:

There are minor changes/additions/revisions to the Information Security Management System (ISMS) framework (Clauses 4 to 10). ControlCase considers changes within the body of the ISO 27001 standard that have been made to better align with the harmonized structure for management system standards (i.e., Annex SL).

The Annex A controls have been regrouped from 14 control objectives to 4 broad themes: Organizational, People, Physical, and Technological Controls. The overall number of controls within Annex A stands at 93 controls compared to the 114 controls in the previous edition.

To ensure that clients are successful with their transition, ControlCase advises the following steps:

Preparing for your ISO 27001:2022 Transition:

- Organizations must transition their existing *management system* in accordance with the requirements to ISO 27001:2022 before their transition audit is conducted. This should include gap analysis, any documentation changes, review of risk assessment & treatment results, review of SOA, training of employees, and evidence of any new or changed process requirements.
- Organizations must conduct an *internal audit and management review* of the new/changed requirements before the ControlCase transition audit is conducted.

Your ISO 27001:2022 Transition Audit:

- All organizations must have a transition audit to confirm the implementation of the revised standard. The transition audit may be conducted in conjunction with an existing audit or may be a stand-alone audit.
- If the transition audit is conducted in conjunction with existing surveillance (i.e., transition surveillance) or recertification audit (i.e., transition re-assessment), additional time may be added to the audit duration to cover the new requirements/concepts introduced by ISO 27001:2022.
- If a stand-alone audit is carried out for the transition audit, the duration be calculated on an individual organization basis.

Note: *Specific audit durations for transition will depend on the actual situation of the organization, including the organization's size and the complexity of the ISMS. Your ControlCase Client representative will advise you of your specific transition audit duration. *Per IAD MD 26 Transition requirements for ISOIEC 27001:2022, 1) Minimum of 0.5 auditor days for the transition audit when carried out along with a recertification audit. 2) Minimum of 1.0 auditor days for the transition audit when carried out along with a surveillance audit or as a separate audit.*

Revised ISO 27001:2022 Certificates:

- Non-conformances identified during a transition audit require a corrective action plan(s) to be submitted and approved. An updated ISO 27001:2022 certificate will be issued following the approval of the corrective action plan (s).
- Updated ISO 27001:2022 certificate issuance and validity will be as follows:

    - ✓ *Transition surveillance* – The organization's existing 'Valid Until Date' will be maintained.
    - ✓ *Transition re-assessment* – A new 'Valid Until Date' will be issued for the renewed 3-year period.
    - ✓ *Stand-alone transition* – The organization's existing 'Valid Until Date' will be maintained.